

**DEFENDANT CISCO SYSTEMS, INC.’S RULE 12(C) MOTION
FOR JUDGMENT ON THE PLEADINGS**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	5
II. LEGAL STANDARDS	5
A. Motion for Judgment on the Pleadings Standards	5
B. Direct Infringement Standards	6
III. THE PATENTS-IN-SUIT	8
A. The '442 Patent	8
B. The '614 Patent	9
C. The '470 Patent	9
D. The '974 Patent	10
IV. THE ACCUSED SYSTEM	10
V. CTD FAILS TO STATE A PLAUSIBLE CLAIM FOR INFRINGEMENT OF THE PATENTS-IN-SUIT.	11
A. No Cisco Product Infringes the '442 Patent.	12
B. No Cisco Product Infringes the '614 Patent.	13
C. No Cisco Product Infringes the '470 Patent.	14
D. No Cisco Product Infringes the '974 Patent.	15
E. CTD's Attempt to Improperly Mix-and-Match Different Products for the Same Claim Should Be Rejected.	15
VI. CONCLUSION.....	16

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	<i>passim</i>
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	14, 15, 16
<i>Bot M8 LLC v. Sony Corp. of Am.</i> , 4 F.4th 1342 (Fed. Cir. 2021)	8
<i>Bowlby v. City of Aberdeen</i> , 681 F.3d 215 (5th Cir. 2012)	7
<i>CAP Co. v. McAfee, Inc.</i> , No. 14-cv-05068-JD, 2015 U.S. Dist. LEXIS 104697 (N.D. Cal. Aug. 10, 2015)	7, 17
<i>Chhim v. Univ. of Tex. At Austin</i> , 836 F.3d 467 (5th Cir. 2016)	8, 14, 15, 16
<i>De La Vega v. Microsoft Corp.</i> , No. 6:19-cv-00612-ADA, 2020 U.S. Dist. LEXIS 116081 (W.D. Tex. Feb. 7, 2020)	8
<i>Encoditech, LLC v. Citizen Watch Co. of Am., Inc.</i> , No. SA-18-CV-1335-XR, 2019 U.S. Dist. LEXIS 105833 (W.D. Tex. June 25, 2019)	7
<i>Free Motion Fitness, Inc. v. Cybex Int’l, Inc.</i> , 311 F. Supp. 2d 1297 (D. Utah 2003).....	8, 17
<i>Geovector Corp. v. Samsung Elecs. Co.</i> , No. 16-cv-02463-WHO, 2017 U.S. Dist. LEXIS 3626 (N.D. Cal. Jan. 9, 2017).....	<i>passim</i>
<i>Gonza LLC v. Mission Competition Fitness Equip. LLC</i> , No. W-21-CV-00771-ADA, 2021 U.S. Dist. LEXIS 229632 (W.D. Tex. Dec. 1, 2021)	7
<i>Great Plains Tr. Co. v. Morgan Stanley Dean Witter & Co.</i> , 313 F.3d 305 (5th Cir. 2002)	6
<i>LifeNet Health v. LifeCell Corp.</i> , 837 F.3d 1316 (Fed. Cir. 2016).....	7

<i>Lone Star Fund V (U.S.) L.P. v. Barclays Bank PLC</i> , 594 F.3d 383 (5th Cir. 2010)	6
<i>Uniloc 2017 LLC v. Apple, Inc.</i> , No. 19-cv-01904-WHO, 2019 U.S. Dist. LEXIS 230501 (N.D. Cal. Dec. 16, 2019)	8, 17
<i>Vervain, LLC v. Micron Tech., Inc.</i> , No. 6:21-CV-00487-ADA, 2022 U.S. Dist. LEXIS 54 (W.D. Tex. Jan. 3, 2022)	8
<i>Zitovault v. IBM</i> , No. 3:16-cv-0962-M, 2018 U.S. Dist. LEXIS 234540 (N.D. Tex. Mar. 29, 2018)	<i>passim</i>

Statutes

35 U.S.C. § 271(a)	7
--------------------------	---

Other Authorities

Federal Rule of Civil Procedure 12(c)	6
https://www.cisco.com/c/en/us/solutions/cloud/index.html	11
U.S. Patent Nos. 8,327,442	6, 9, 10, 13

I. INTRODUCTION

Plaintiff CTD Networks LLC’s (“CTD”) filed its Original Complaint and demand for jury trial against Cisco Systems, Inc. (“Cisco”), alleging infringement of U.S. Patent Nos. 8,327,442 (“the ’442 Patent”), 9,438,614 (“the ’614 Patent”), 9,503,470 (“the ’470 Patent”), 11,171,974 (“the ’974 Patent”) (collectively, the “Patents-in-Suit”). Cisco filed its Answer to the Original Complaint on December 29, 2022, asserting defenses. Because CTD has not actually accused any single Cisco product of infringing any asserted patent claim, and thus has not set forth a plausible claim of infringement, Cisco hereby moves for judgment on the pleadings. Based on this motion, Cisco respectfully requests that the Court dismiss with CTD’s complaint with prejudice.

II. LEGAL STANDARDS

A. Motion for Judgment on the Pleadings Standards

A motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c) is “designed to dispose of cases where the material facts are not in dispute and a judgment on the merits can be rendered by looking to the substance of the pleadings and any judicially noticed facts.” *Great Plains Tr. Co. v. Morgan Stanley Dean Witter & Co.*, 313 F.3d 305, 312 (5th Cir. 2002) (internal quotation marks omitted). In order to survive a 12(c) motion, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is not plausible unless the “plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Twombly*, 550 U.S. at 556). In making this assessment, courts may consider “the complaint, any documents attached to the complaint, and any documents attached to the motion to dismiss that are central to the claim and referenced by the complaint.” *Lone Star Fund V (U.S.) L.P. v. Barclays Bank PLC*, 594 F.3d 383, 387 (5th Cir. 2010). The court must then decide whether

those facts state a claim for relief that is plausible on its face. *Bowlby v. City of Aberdeen*, 681 F.3d 215, 219 (5th Cir. 2012). While factual allegations set out in the pleadings should be taken in the light most favorable to the nonmoving party, courts “are not bound to accept as true a legal conclusion couched as a factual allegation,” and “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice” to meet the plausibility standard. *Ashcroft*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555).

B. Direct Infringement Standards

To state a viable claim for direct infringement under 35 U.S.C. § 271(a), a “plaintiff must plead facts that plausibly suggest that the accused product meets each limitation of the asserted claim or claims.” *See Encoditech, LLC v. Citizen Watch Co. of Am., Inc.*, No. SA-18-CV-1335-XR, 2019 U.S. Dist. LEXIS 105833, at *9 (W.D. Tex. June 25, 2019) For apparatus or system claims, direct infringement “requires that each and every limitation set forth in a claim appear in an accused product.” *LifeNet Health v. LifeCell Corp.*, 837 F.3d 1316, 1325 (Fed. Cir. 2016) (quoting *Cross Med. Prods., Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1310 (Fed. Cir. 2005)); *see also Gonza LLC v. Mission Competition Fitness Equip. LLC*, No. W-21-CV-00771-ADA, 2021 U.S. Dist. LEXIS 229632, at *5 (W.D. Tex. Dec. 1, 2021) (quoting *Johnston v. IVAC Corp.*, 885 F.2d 1574, 1577 (Fed. Cir. 1989)) (“To establish infringement of a patent, every limitation set forth in a claim must be found in an accused product or process exactly or by a substantial equivalent.”).

Importantly, “[i]nfringement cannot be shown by a muddled hash of elements from different products, since in order to infringe, ‘the accused device must contain each limitation of the claim, either literally or by an equivalent.’” *CAP Co. v. McAfee, Inc.*, No. 14-cv-05068-JD, 2015 U.S. Dist. LEXIS 104697, at *5 (N.D. Cal. Aug. 10, 2015) (quoting *TecSec, Inc. v. Int'l Business Machines Corp.*, 731 F.3d 1336, 1351 (Fed. Cir. 2013)). Therefore, a plaintiff must, “at

a minimum, ‘chart a *single product* against all elements.’ A plaintiff *does not satisfy this requirement by ‘mixing and matching between different accused products’* in its claim charts.” *Geovector Corp. v. Samsung Elecs. Co.*, No. 16-cv-02463-WHO, 2017 U.S. Dist. LEXIS 3626, at *11 (N.D. Cal. Jan. 9, 2017) (quoting *CAP*, 2015 U.S. Dist. LEXIS 104697, at *5) (emphasis added); *see also Zitovault v. IBM*, No. 3:16-cv-0962-M, 2018 U.S. Dist. LEXIS 234540, at *9 (N.D. Tex. Mar. 29, 2018) (stating it would be improper to “only chart [one product’s] functionality for some limitations and [another product’s] functionality for other limitations”); *Free Motion Fitness, Inc. v. Cybex Int’l, Inc.*, 311 F. Supp. 2d 1297, 1306 (D. Utah 2003) (granting summary judgement for non-infringement because the plaintiff did not show that “each of the accused devices” contained all elements of the asserted claim); *Uniloc 2017 LLC v. Apple, Inc.*, No. 19-cv-01904-WHO, 2019 U.S. Dist. LEXIS 230501, at *16 (N.D. Cal. Dec. 16, 2019).

Further, a plaintiff cannot satisfy the *Iqbal/Twombly* standard “by reciting the claim elements and merely concluding that the accused product has those elements. There must be some factual allegations that, when taken as true, articulate why it is plausible that the accused product infringes the patent claim.” *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1353 (Fed. Cir. 2021). When the complaint fails to allege that the defendant satisfies each element of the claim, claims of direct infringement are not plausible and should be dismissed. *See De La Vega v. Microsoft Corp.*, No. 6:19-cv-00612-ADA, 2020 U.S. Dist. LEXIS 116081, at *5-18 (W.D. Tex. Feb. 7, 2020). A conclusory recitation that “merely track[s] the claim language” is “insufficient to give rise to a reasonable inference” of infringement. *Vervain, LLC v. Micron Tech., Inc.*, No. 6:21-CV-00487-ADA, 2022 U.S. Dist. LEXIS 54, at *20 (W.D. Tex. Jan. 3, 2022) (quoting *Bot M8 LLC v. Sony Corp.*, 4 F.4th 1342, 1355 (Fed. Cir. 2021)); *see also Chhim v. Univ. of Tex. At Austin*, 836 F.3d

467, 469 (5th Cir. 2016) (“[W]e do not credit conclusory allegations or allegations that merely restate the legal elements of a claim.”).

III. THE PATENTS-IN-SUIT

A. The '442 Patent

The '442 Patent, entitled “System and method for a distributed application and network security system (SDI-SCAM),” discloses the architecture and proposed application of a highly distributed network security system that serves to detect, prevent, and repair a wide variety of network intrusions. '442 Patent at Abstract, Dkt. 1-1, Ex. A. The '442 Patent acknowledges a well-known problem that “[c]omputer networks today are as vulnerable as ever from unauthorized intrusions by external entities.” *Id.* at 1:21-22. Therefore, it proposes an architecture to “protects computers at individual client locations, but which constantly pools and analyzes information gathered from machines across a network in order to quickly detect patterns consistent with intrusion or attack, singular or coordinated.” *Id.* at 1:47-52. Claim 1, which is the only charted '442 claim in CTD's Complaint, recites as follows:

1. A distributed security system that protects individual computers in a computer network having a plurality of computers, said system comprising individual computers having agents associated therewith that control the associated individual computer, each agent performing the steps of:
 - creating statistical models of usage of the associated individual computer in said computer network;
 - gathering and analyzing information relating to current usage of the associated individual computer in said computer network;
 - determining from said information a pattern of usage of the associated individual computer that is consistent with intrusion or attack of the associated individual computer or the computer network;
 - determining a probability of the likelihood of an intrusion or attack from said pattern of usage of the associated individual computer;
 - distributing in real-time warnings and potential countermeasures to agents of each of said individual computers in said computer network when the determined probability of the likelihood of an intrusion or attack exceeds a statistical threshold, wherein at least one of said warnings comprises information related to the nature of the intrusion or attack and the determined probability of

the likelihood of intrusion or attack based on the statistical models of the associated individual computer; and

updating said statistical models of the associated individual computer to reflect the current usage of the associated individual computer in said computer network and the likelihood of intrusion or attack;

wherein each said agent schedules the associated individual computers for different anti-viral software updates based on different levels of probability of an intrusion or attack for each individual computer based on the statistical model for each individual computer and a detected level of probability of an intrusion or attack; and

wherein each said agent suspends said schedule and immediately provides the anti-viral software update to the associated individual computer when an intrusion or attack of any computer in said computer network is detected or the detected probability of an intrusion or attack is high that the associated individual computer has been infected by a particular type of virus.

Id. at 15:51-16:26.

B. The '614 Patent

The '614 Patent, entitled "SDI-SCAM," is similar to the '442 Patent in that it "relates to a system and method for detecting the condition of a computer network and identifying threats to the network using passive data analysis techniques." '614 Patent at 1:14-17, Dkt. 1-1, Ex. B. Also, like claim 1 of the '442 Patent, claim 10 of the '614 Patent, which is the only charted '614 claim in the Complaint, recites a "system that detects the state of a computer network having a plurality of nodes" and "comprising a plurality of distributed agents designed for adaptive learning and probabilistic analysis." *Id.* at 19:33-46.

C. The '470 Patent

The '470 Patent, entitled "Distributed agent based model for security monitoring and response," resulted from a continuation-in-part (CIP) application of the '442 Patent. '470 Patent, Cover, Dkt. 1-1. Like the '442 Patent, the '470 Patent "related to the field of security systems for computer networks." '470 Patent at 1:22-23, Dkt. 1-1, Ex. C. Also, like claim 1 of the '442 Patent, claim 1 of the '470 Patent, which is the only charted '470 claim in the Complaint, recites a "system that detects the state of a computer network, comprising a plurality of distributed agents disposed

in said computer network” and “a server that provides a security and validity score for free software available for download.” *Id.* at 28:9-39.

D. The '974 Patent

The '974 Patent, entitled the same as the '470 Patent, is a continuation of the '470 Patent. '974 Patent, Cover, Dkt. 1-1, Ex. D. Like claim 1 of the '470 Patent, claim 1 of the '974 Patent, which is the only charted '974 claim in the Complaint, recites a “system that detects the state of a computer network, comprising a plurality of distributed agents disposed in said computer network.” *Id.* at 28:5-36.

IV. THE ACCUSED SYSTEM

CTD alleges that the “Cisco Cloud Solutions system” is the “Accused Products” that infringe the Patents-in-Suit. Compl. ¶ 18, Dkt. 1. CTD attaches four claim charts to the Complaint to describe how Cisco Cloud Solutions infringe one exemplary claim from each of the four Patent-in-Suit. *Id.* ¶ 27 (citing Exhibit E for claim 1 of the '442 Patent), ¶ 36 (citing Exhibit F for claim 10 of the '614 Patent), ¶ 45 (citing Exhibit G for claim 1 of the '470 Patent), ¶ 52 (citing Exhibit H for claim 1 of the '974 Patent).¹

First, as is clear from the first Cisco webpage referenced on the first page of every claim chart, the term “Cisco Cloud Solutions system” is manufactured by Plaintiff, and does not refer to any actual Cisco product. Instead, Plaintiff uses the term “Cisco Cloud Solutions system” to refer to a wide variety of different “products,” “use cases,” “case studies,” and “resources” offered by Cisco or discussed in Cisco literature. *See, e.g., id.* Ex. E at 1 (referencing webpage at link <https://www.cisco.com/c/en/us/solutions/cloud/index.html>, which is attached here as **Exhibit 1**). For example, clicking the “Products” button on this webpage will lead one to a wide variety of

¹ All charted claims of the Patents-in-Suit are system claims, and no method claims were charted.

different products under three categories “networking,” “security,” and “app and workload management.” There is no indication, either in the cited materials, or in Plaintiff’s allegations, that these different products are part of a single system or product, or are inter-operable to form a “system.”

In fact, CTD’s four claim charts cite at least 10 different products in a mix-and-match fashion, with different products cited for different limitations of a single claim, including: Cisco Secure Cloud Analytics (also known as Stealthwatch), Cisco Secure Workload (also known as Tetration), Industrial Automation Solution, Email Security Appliance, Security Intelligence Operations, CX Cloud Agent, Secure Cloud for AWS, ThousandEyes, SecureX platform, Secure Web Appliance, and Secure Email Cloud Gateway. Compl. Exs. E, F, G, H, Dkt. 1-1 at 69-122. Yet, CTD cites no evidence that these charted products are *all* part of the accused “Cisco Cloud Solutions.”

V. CTD FAILS TO STATE A PLAUSIBLE CLAIM FOR INFRINGEMENT OF THE PATENTS-IN-SUIT.

The Court should grant Cisco’s 12(c) motion because CTD’s Complaint fails to show how any single Cisco product infringes any claims of the Patents-in-Suit. CTD does not chart any single Cisco product against all elements of any claim. Instead, as shown in the table below and further explained below, CTD engages in improper “mixing and matching between different accused products” by arbitrarily citing documentation from many different Cisco products. *Geovector*, 2017 U.S. Dist. LEXIS 3626, at *11. The table below summarizes the different products being charted against each element of each asserted claim of the Patents-in-Suit (Compl. Exs. E, F, G, H, Dkt. 1-1 at 69-122):

Claim Element	Charted Product(s)
’442 Elements 1a, 1b, 1d	Secure Cloud Analytics, Secure Workload
’442 Element 1c	Secure Workload, Industrial Automation Solution

'442 Element 1e	Email Security Appliance
'442 Element 1f	Secure Cloud Analytics, Email Security Appliance
'442 Element 1g	Secure Cloud Analytics
'442 Elements 1h, 1i	Security Intelligence Operations
'614 Element 10a	Secure Cloud Analytics
'614 Element 10b	CX Cloud Agent, Secure Workload, and a blog webpage unrelated to any product
'614 Element 10c	Secure Workload, Industrial Automation Solution, Secure Cloud for AWS
'614 Element 10d	Secure Cloud Analytics, Secure Workload
'614 Elements 10e, 10f	Email Security Appliance
'470 Elements 1a, 1e	Secure Cloud Analytics
'470 Element 1b	Secure Workload
'470 Element 1c	Secure Workload, Industrial Automation Solution
'470 Element 1d	Secure Cloud Analytics, Secure Workload
'470 Element 1f	Secure Workload, Industrial Automation Solution, Secure Cloud for AWS
'470 Element 1g	Secure Cloud for AWS
'470 Element 1h	ThousandEyes
'470 Element 1i	SecureX platform, Secure Web Appliance, Secure Email Cloud Gateway
'974 Elements 1a, 1e	Secure Cloud Analytics
'974 Element 1b	Secure Workload
'974 Element 1c	Secure Workload, Industrial Automation Solution
'974 Elements 1d, 1f	Secure Cloud Analytics, Secure Workload
'974 Element 1g	Email Security Appliance
'974 Element 1h	Secure Workload, Industrial Automation Solution, Secure Cloud for AWS
'974 Element 1i	Security Intelligence Operations

A. No Cisco Product Infringes the '442 Patent.

As shown in the table above, CTD arbitrarily cites documentation from at least five different Cisco products for claim 1 of the '442 Patent, including Secure Cloud Analytics, Secure Workload, Industrial Automation Solution, Email Security Appliance, and Security Intelligence Operations. Compl. Ex. E at 1-15, Dkt. 1-1 at 69-83. No single Cisco product is charted against all elements of claim 1. Far from it. For example, CTD cites only Email Security Appliance for element 1e (*id.* at 7), cites only Secure Cloud Analytics for element 1g (*id.* at 9), and cites only

Security Intelligence Operations for elements 1h and 1i (*id.* at 9-15). These are all different products. Even assuming *arguendo* that CTD wished to contend that the five products are all part of a “Cisco Cloud Solution,” CTD must cite sufficient evidence that their accused functionalities all work together as related parts of an integrated system. *Geovector*, 2017 U.S. Dist. LEXIS 3626, at *11; *Zitovault*, 2018 U.S. Dist. LEXIS 234540, at *9. Unsurprisingly, CTD cites no such evidence. And even if CTD has offered conclusory statements, those would be insufficient to satisfy the *Iqbal* / *Twombly* standard. *Chhim*, 836 F.3d at 469.²

B. No Cisco Product Infringes the ’614 Patent.

As shown in the table above, CTD arbitrarily cites documentation from at least six different Cisco products for claim 10 of the ’614 Patent, including Secure Cloud Analytics, CX Cloud Agent, Secure Workload, Industrial Automation Solution, Secure Cloud for AWS, and Email Security Appliance. Compl. Ex. F at 1-8, Dkt. 1-1 at 85-92. No single Cisco product is charted against all elements of claim 10. For example, CTD cites only Secure Cloud Analytics for claim element 10a (*id.* at 1-2), cites only Secure Workload, Industrial Automation Solution, and Secure Cloud for AWS for element 10c (*id.* at 4-5), and cites only Email Security Appliance for elements 10e and 10f (*id.* at 7-8). These are all different, non-overlapping products. Even assuming *arguendo* that CTD wished to contend that the six products are all part of a “Cisco Cloud Solution,” CTD must cite sufficient evidence that their accused functionalities all work together as related parts of an integrated system. *Geovector*, 2017 U.S. Dist. LEXIS 3626, at *11; *Zitovault*, 2018 U.S. Dist. LEXIS 234540, at *9. CTD cites no such evidence. Even if CTD had made a conclusory

²For many products such as Industrial Automation Solution and Email Security Appliance, CTD’s Complaint lacks even conclusory statements that they are part of the Cisco Cloud Solutions. *See, e.g.*, Compl. Ex. E at 4-5, 7.

allegation that the products work together to form the “Cisco Cloud Solution,” this would still not satisfy the *Iqbal* / *Twombly* standard. *Chhim*, 836 F.3d at 469.³

C. No Cisco Product Infringes the ’470 Patent.

As shown in the table above, CTD arbitrarily cites documentation from at least eight different Cisco products for claim 1 of the ’470 Patent, including the Secure Cloud Analytics, Secure Workload, Industrial Automation Solution, Secure Cloud for AWS, ThousandEyes, SecureX platform, Secure Web Appliance, and Secure Email Cloud Gateway. Compl. Ex. G at 1-15, Dkt. 1-1 at 94-108. No single Cisco product is charted against all elements of claim 1. For example, CTD cites only Secure Cloud Analytics for claim elements 1a and 1e (*id.* at 1-2, 6-7), cites only Secure Workload for element 1b (*id.* at 2-3), cites only Secure Cloud for AWS for element 1g (*id.* at 10-11), cites only ThousandEyes for element 1h (*id.* at 12-14), and cites only SecureX platform, Secure Web Appliance, and Secure Email Cloud Gateway for element 1i (*id.* at 15). These are all different, non-overlapping products. Even assuming *arguendo* that CTD wished to contend that the six products are all part of a “Cisco Cloud Solution,” CTD must cite sufficient evidence that their accused functionalities all work together as related parts of an integrated system. *Geovector*, 2017 U.S. Dist. LEXIS 3626, at *11; *Zitovault*, 2018 U.S. Dist. LEXIS 234540, at *9. CTD cites no such evidence. Even if CTD had made a conclusory allegation that the products work together to form the “Cisco Cloud Solution,” this would still not satisfy the *Iqbal* / *Twombly* standard. *Chhim*, 836 F.3d at 469.⁴

³For many products such as Industrial Automation Solution, Secure Cloud for AWS, and Email Security Appliance, CTD’s Complaint lacks even conclusory statements that they are part of the Cisco Cloud Solutions. *See, e.g.*, Compl. Ex. F at 4-5.

⁴For many products such as Industrial Automation Solution, Secure Cloud for AWS, ThousandEyes, Secure Web Appliance, and Secure Email Cloud Gateway, CTD’s Complaint lacks even conclusory statements that they are part of the Cisco Cloud Solutions. *See, e.g.*, Compl. Ex. G at 3, 10-15. Indeed, CTD admits that the Secure Web Appliance and Secure Email Cloud Gateway are “[o]ther Cisco services” separate from “Cisco Cloud Solutions.” *Id.* at 15.

D. No Cisco Product Infringes the '974 Patent.

As shown in the table above, CTD arbitrarily cites documentation from at least six different Cisco products for claim 1 of the '974 Patent, including the Secure Cloud Analytics, Secure Workload, Industrial Automation Solution, Email Security Appliance, Secure Cloud for AWS, and Security Intelligence Operations. Compl. Ex. H at 1-13, Dkt. 1-1 at 110-22. No single Cisco product is charted against all elements of claim 1. For example, CTD cites only Secure Cloud Analytics for claim elements 1a and 1e (*id.* at 1-2, 6-7), cites only Secure Workload for element 1b (*id.* at 2-3), cites only Email Security Appliance for element 1g (*id.* at 9-10), and cites only Security Intelligence Operations for element 1i (*id.* at 12-13). These are all different, non-overlapping products. Even assuming *arguendo* that CTD wished to contend that the six products are all part of a “Cisco Cloud Solution,” CTD must cite sufficient evidence that their accused functionalities all work together as related parts of an integrated system. *Geovector*, 2017 U.S. Dist. LEXIS 3626, at *11; *Zitovault*, 2018 U.S. Dist. LEXIS 234540, at *9. CTD cites no such evidence. Even if CTD had made a conclusory allegation that the products work together to form the “Cisco Cloud Solution,” this would still not satisfy the *Iqbal* / *Twombly* standard. *Chhim*, 836 F.3d at 469.⁵

E. CTD’s Attempt to Improperly Mix-and-Match Different Products for the Same Claim Should Be Rejected.

As discussed above, CTD has failed to meet its burden to “at a minimum, ‘chart a single product against all elements’” of an asserted claim. *Geovector*, 2017 U.S. Dist. LEXIS 3626, at *11 (quoting *CAP*, 2015 U.S. Dist. LEXIS 104697, at *5). Rather, for each asserted claim of the Patents-in-Suit, CTD has engaged in improper “mixing and matching between different accused

⁵For many products such as Industrial Automation Solution, Email Security Appliance, and Secure Cloud for AWS, CTD’s Complaint lacks even conclusory statements that they are part of the Cisco Cloud Solutions. *See, e.g.*, Compl. Ex. H at 3, 9-10.

products” for elements of the same claim. *Id.* For example, CTD only charts one product’s functionality for some claim elements and another product’s functionality for other claim elements. *Zitovault*, 2018 U.S. Dist. LEXIS 234540, at *9. Such an attempt must be rejected because “[i]nfringement cannot be shown by a muddled hash of elements from different products” and one accused product “must contain each limitation of the claim.” *CAP*, 2015 U.S. Dist. LEXIS 104697, at *5 (quoting *TecSec*, 731 F.3d at 1351); *see also Free Motion Fitness*, 311 F. Supp. 2d at 1306; *Uniloc 2017 LLC*, 2019 U.S. Dist. LEXIS 230501, at *16. Therefore, CTD has failed to show that any actual Cisco product plausibly infringes any asserted claim of the Patents-in-Suit.

VI. CONCLUSION.

For the reasons stated above, Defendant Cisco respectfully requests that the Court dismiss CTD’s claims of infringement with respect to all Patents-in-Suit with prejudice.

DATED: February 3, 2023

Respectfully Submitted,

By : /s/ Krishnan Padmanabhan
Krishnan Padmanabhan
kpadmanabhan@winston.com
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: 212-294-6700
Facsimile: 212-294-4700

Barry K. Shelton
Texas Bar No. 24055029
Winston & Strawn LLP
2121 N. Pearl Street, Suite 900
Dallas, TX 75201
Telephone: (214) 453-6407
Facsimile: (214) 453-6400
bshelton@winston.com

Chaoxuan Charles Liu
Texas Bar No. 24100410
WINSTON & STRAWN LLP
2121 N. Pearl Street, Suite 900
Dallas, TX 75201
Telephone: (214) 453-6423
Facsimile: (214) 453-6400
ccliu@winston.com

ATTORNEYS FOR DEFENDANT
CISCO SYSTEMS, INC.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the above document has been served on February 3, 2023 to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system per the Local Rules.

s/ Krishnan Padmanabhan
Krishnan Padmanabhan